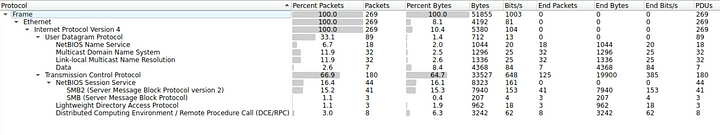
### **PoisonedCredentials Lab — CyberDefenders**

**Scenario:** Your organization’s security team has detected a surge in suspicious network activity. There are concerns that LLMNR (Link-Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) poisoning attacks may be occurring within your network. These attacks are known for exploiting these protocols to intercept network traffic and potentially compromise user credentials. Your task is to investigate the network logs and examine captured network traffic.

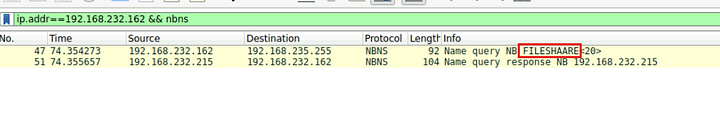
TASKS



1. **In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistyped query made by the machine with the IP address 192.168.232.162?**

We can look for the NBNS packets to and from the above mentioned IP address using the following filter.

ip.addr==192.168.232.162 && nbns

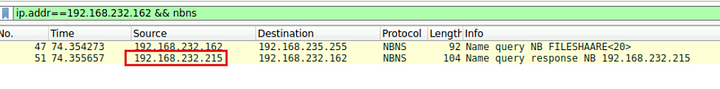


Above, we can see the NBNS request made by the machine and the corresponding response.

**Answer:** FILESHAARE

**2. We are investigating a network security incident. To conduct a thorough investigation, We need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity?**

Usually, when a host requests a non existent name, there will not be any response and the request will timeout after a while. But as we see in the above screenshot, the user actually got a response from 192.168.232.215. From this we can confirm that this IP address is the rogue entity.

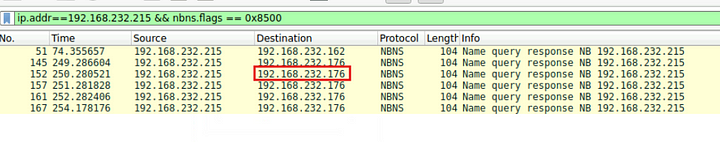


**Answer:** 192.168.232.215

**3. As part of our investigation, identifying all affected machines is essential. What is the IP address of the second machine that received poisoned responses from the rogue machine?**

Now that we know the rogue entity, we can search for all the NBNS responses this entity sent, to find out other affected machines.

ip.addr==192.168.232.215 && nbns.flags == 0x8500

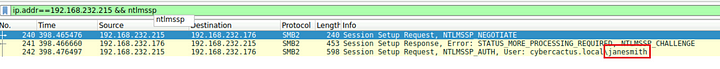


**Answer:** 192.168.232.176

**4. We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised?**

Since there is NTLMSSP related packets in the captured traffic, we can filter for these packets and the attacker IP address. This will display any authentications attempts made by the attacker.

ip.addr==192.168.232.215 && ntlmssp

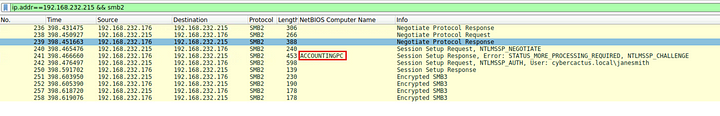


**Answer:** janesmith

**5. As part of our investigation, we aim to understand the extent of the attacker’s activities. What is the hostname of the machine that the attacker accessed via SMB?**

We can look for the SMB packets related to the attacker IP. Specifically we can look for the NTLM challenge packets, which will contain the name of the machine.

ip.addr==192.168.232.215 && smb2



**Answer:** ACCOUNTINGPC

This is the end of the walkthrough.